

Secured File Transfer Server Implementation

AHCCCS will be implementing a new Secure File Transfer Server (SFTS) server on **June 18, 2009**. The new SFTS server will replace the current server used to send / receive files from AHCCCS.

SFTP server properties:

- A Virtual Private Network (VPN) connection will no longer be required to connect to AHCCCS. No additional software is required.
- The SFTS server accepts a standard web browser via HTTPS and FTP over SSH (SFTP)
- Service Accounts will be used by trading partners for their automated processes. These accounts will be linked to one IP address provided by the trading partner.
- Individuals must receive their own user account to access the SFTS server, no generic accounts will be allowed.
- Folder structures have been simplified. High level folders will be name:
 - **Dev** - for internal AHCCCS development staff
 - **Other** - for sending / receiving large files that cannot be sent in an email or contains PHI.
 - **Prod** -for sending / receiving production files
 - **Test** - for sending / receiving test files
 - Under the Dev, Prod and Test folders, the following folders will be defined:
 - **EDI-IN** for sending HIPAA X12 and NCPDP 5.1 transaction files only. Zipped files will not be allowed
 - **EDI-OUT** for receiving HIPAA X12 transactions only
 - **IN** for sending proprietary files
 - **OUT** for receiving proprietary files
- Files will be removed automatically after 90 days
- Website is <https://sftp.statemedicaid.us/>
- SFTP site is sftp.statemedicaid.us on port 22

To obtain new User IDs and passwords, please complete and submit the "Electronic Data Exchange Form" that is located on the AHCCCS Website at: <http://www.azahcccs.gov/PlansProviders/Forms.asp>

Send questions or issues to: EDICustomerSupport@azahcccs.gov